UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN

DOUGLAS DINNING, individually and on behalf of all others similarly situated, Plaintiff, v. HEALTHEC LLC, COREWELL HEALTH, and OAKWOOD ACCOUNTABLE CARE ORGANIZATION, LLC d/b/a BEAUMONT ACO Defendants.	Case No. _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Douglas Dinning ("Plaintiff") brings this Class Action Complaint ("Complaint") against Defendants HealthEC LLC ("HEC"), Corewell Health ("Corewell"), and Oakwood Accountable Care Organization d/b/a Beaumont ACO ("BACO") (collectively, "Defendants"), as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsel's investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This class action arises out of the July 2023 cyberattack and data breach resulting from Defendants' combined failure to implement reasonable and industry

standard data security practices.

2. Defendant Corewell is a network of health systems that offers healthcare services in Michigan.

3. Defendant BACO is an accountable care organization.

4. Defendant HEC is a population health management platform that provides services to health systems and care organizations, including Corewell and BACO.

5. Defendants collected and maintained certain personally identifiable information and/or protected health information of Plaintiff and the putative Class Members (defined below).

6. Between July 14, 2023 and July 23, 2023, HEC's data information systems were illicitly accessed, which included access to files containing personal information about Corewell, BACO, and other health systems and care organizations' current and former patients (the "Data Breach").

7. Plaintiff's and Class Members' sensitive personal information—which they entrusted to Defendants on the mutual understanding that Defendants would protect it against disclosure—was compromised and illicitly accessed due to the Data Breach.

8. The Private Information compromised in the Data Breach included Plaintiff's and Class Members' personally identifiable information ("PII") and

protected health information ("PHI", and collectively with PII, "Private Information" or "PII/PHI") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The Private Information included names, addresses, dates of birth, Social Security numbers, Taxpayer Identification numbers, medical record numbers, medical information (including but not limited to diagnoses, diagnosis codes, mental/physical conditions, prescription information, and provider names and locations), health insurance information (including but not limited to beneficiary numbers, subscriber numbers, Medicaid/Medicare identifications), and/or billing and claims information (including but not limited to patient account numbers, patient identification numbers, and treatment cost information) that Defendants collected and maintained as part of their provision of services.[1]

9. The Private Information compromised in the Data Breach was exfiltrated by cyber-criminals and remains in the hands of those cyber-criminals who target Private Information for its value to identity thieves.

10. As a result of the Data Breach, Plaintiff and approximately one million Class Members[2] suffered concrete injuries in fact including, but not limited to: (i)

[1] Notice of HealthEC LLC Cybersecurity Event ("Notice of Data Breach"), available at https://www.healthec.com/cyber-incident/ (last accessed Jan. 4, 2024) (attached as **Exhibit A** hereto).

[2] *1 Million Corewell Health Patients Could be Impacted by Second Data Breach*, MLive, Michael Kransz (Dec. 26, 2023), https://www.mlive.com/news/ann-

invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; and (vi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

11. The Data Breach was a direct result of Defendants' failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Plaintiff's and putative Class Members' Private Information from a foreseeable and preventable cyber-attack.

12. Defendants maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on HEC's computer network and data systems in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to

---

arbor/2023/12/1-million-corewell-health-patients-could-be-impacted-by-second-data-breach.html (last accessed Jan. 4, 2024) (attached as **Exhibit B** hereto).

Defendants, and, thus, Defendants were on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

13. Defendants disregarded the rights of Plaintiff and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure HEC's computer network and data systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

14. Defendants' negligent conduct has put Plaintiff's and Class Members' Private Information now at risk because this Private Information that Defendants collected and maintained is now in the hands of data thieves who illicitly obtained this Private Information.

15. Armed with the Private Information accessed in the Data Breach, data thieves have already engaged in identity theft and fraud and can in the future commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns

using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

16. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

17. Plaintiff and Class Members may also incur out of pocket costs, e.g., for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

18. Plaintiff brings this class action lawsuit on behalf all those similarly situated to address Defendants' inadequate safeguarding of Class Members' Private Information that Defendants collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access by an unknown third party and precisely what specific type of information was accessed.

19. Plaintiff's claims are brought as a class action, pursuant to Federal Rule of Civil Procedure 23, on behalf of himself and all other similarly situated persons. Plaintiff seeks relief in this action individually and on behalf of a similarly situated class of individuals for negligence, breach of implied contract, violations

of the Michigan Consumer Protection Act, violations of the Michigan Data Breach Notification Statute, and unjust enrichment. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

20. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

21. Plaintiff seeks remedies including, but not limited to, compensatory damages and injunctive relief including improvements to Defendants' data security systems and practices, future annual audits, and adequate credit monitoring services funded by Defendants.

PARTIES

Plaintiff Dinning

22. Plaintiff, Douglas Dinning, is a natural person and citizen of Sterling Heights, Michigan, where he intends to remain. Upon information and belief, Plaintiff's PII and/or PHI was compromised in the Data Breach. If Mr. Dinning had known that Defendants would not adequately protect his Private Information, he would not have entrusted Defendants with his Private Information or allowed Defendants to maintain this sensitive Private Information.

Defendant HealthEC LLC

23. Defendant HealthEC LLC, is a limited liability company organized under the state laws of Delaware with its principal place of business located at 343 Thornall Street, Suite 630, Edison, NJ 08837.

Defendant Corewell Health

24. Defendant Corewell Health is a Michigan nonprofit corporation with its headquarters located at 100 Michigan Street Northeast, Grand Rapids, MI 49503.

Defendant Beaumont ACO

25. Defendant Oakwood Accountable Care Organization LLC d/b/a Beaumont ACO is a limited liability company organized under the state laws of Michigan with its headquarters located at 26901 Beaumont Blvd, Southfield, MI 48033.

JURISDICTION AND VENUE

26. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from that of at least one of Defendants.

27. This Court has personal jurisdiction over Defendant HEC because it transacts business within Michigan and makes or performs contracts within Michigan.

28. This Court has personal jurisdiction over Defendant Corewell because it is a Michigan Corporation with its principal place of business and headquarters located in Michigan.

29. This Court has personal jurisdiction over Defendant BACO because it is a Michigan limited liability company with its principal place of business and headquarters located in Michigan.

30. Venue is proper under 28 U.S.C. § 1391(b)(2) because BACO has its headquarters in the Eastern District of Michigan, a substantial part of the events giving rise to Plaintiff's claims arose in this District, and a majority of the harm manifested in this District.

FACTUAL ALLEGATIONS

Background

31. Defendant HEC "is a population health technology company that provides services to other entities."[3] Specifically, HEC "delivers fully integrated analytics and insights that enable value-based health systems and care organizations to identify high-risk patients, close care gaps and recognize barriers to optimal

[3] *See* Notice of Data Breach, *supra* note 1.

care."[4] "More than 1 million healthcare professionals in 18 U.S. states use the platform."[5]

32. Defendant Corewell is a network of health systems that offers connected care across Southeast, Southwest and West Michigan. Corewell "[f]ormed from two leading health systems in Michigan (Beaumont Health and Spectrum Health)" and describes itself as "a not-for-profit health system that provides care and coverage with an exceptional team of 64,000+ dedicated people—including more than 11,500 physicians and advanced practice providers and more than 15,000 nurses offering services in 22 hospitals, 300+ outpatient locations and several post-acute facilities—and Priority Health, a provider-sponsored health plan serving over 1.2 million members across the state of Michigan."[6]

33. Defendant BACO is an accountable care organization, which "is a group of doctors, hospitals, and/or other health care providers who work together to improve the quality and experience of care" patients receive.[7] BACO describes

---

[4] https://www.healthec.com/ (last accessed Jan. 4, 2024) (attached as **Exhibit C**).
[5] *Health EC Data Breach Affects Almost 4.5 Million Individuals*, Steve Alder, The HIPAA Journal (Jan. 3, 2024), https://www.hipaajournal.com/healthec-data-breach/ (last accessed Jan. 4, 2024) (attached as **Exhibit D** hereto).
[6] Who we are, Corewell Health, https://corewellhealth.org/for-michigan-by-michigan (last accessed Jan. 5, 2024) (attached as **Exhibit E** hereto).
[7] Accountable Care Organizations, Medicare.gov, https://www.medicare.gov/manage-your-health/coordinating-your-care/accountable-care-organizations (last accessed Jan. 8, 2024) (attached as

itself as "[a] physician and health system partnership to better position independent, Corewell Health physicians, and hospitals to excel in the new healthcare environment."[8]

34. ACO providers share information, including health records, to coordinate care.[9]

35. In the regular course of their business, Corewell and BACO collect and maintain the Private Information of their current and former patients. Corewell and BACO requires Plaintiff and Class Members to provide their Private Information as a condition of receiving healthcare services from Corewell and BACO.

36. Plaintiff and Class Members are current and former patients of Defendants Corewell and BACO, and entrusted Corewell, BACO, and HEC with their Private Information.

37. Corewell and BACO are "Business Partners/Customers" of HEC.[10]

38. HEC provided services to Defendants Corewell and BACO, which involved Corewell and BACO sharing Plaintiffs' and Class Members' Private Information with HEC.

Exhibit F hereto).

[8] About Beaumont ACO, Beaumont ACO, https://www.beaumont-aco.org/about-us (last accessed Jan. 8, 2024) (attached as **Exhibit G** hereto).

[9] *See* Accountable Care Organizations, *supra* note 7.

[10] *See* Notice of Data Breach, *supra* note 1.

39. Upon information and belief, in the course of collecting Private Information from patients, including Plaintiff, Defendants promised to provide confidentiality and adequate security for patient data through their applicable privacy policies and through other disclosures in compliance with statutory privacy requirements.

40. Indeed, the Privacy Policy posted on Corewell's website provides that: "[t]he privacy of your health information has always been a priority."[11] The Privacy Policy also claims Corewell "understand[s] that health information about you is personal, and we are committed to protecting it."[12]

41. Corewell's Privacy Policy states that it "applies to all of the records related to your care . . . whether electronic or paper, and whether made by hospital personnel, your personal doctor, a consulting or other treating doctor, a diagnostic facility, or any . . . facility or support personnel."[13]

42. Corewell acknowledges that it is required by law to maintain the privacy and security of its patients' Private Information, follow the terms of its Privacy Policy, and notify affected individuals following a data breach.[14]

---

[11] How your health information may be used and disclosed, Corewell Health, https://www.spectrumhealth.org/about-us/patient-privacy (last accessed Jan. 5, 2024) (attached as **Exhibit H** hereto).
[12] *Id.*
[13] *Id.*
[14] *Id.*

43. Corewell claims that it will not use patients' Private Information other than as described in its Privacy Policy without written permission.[15]

44. BACO's Code of Conduct states that BACO is "committed to maintaining the confidentiality and security of personal information obtained throughout the course of the patient's treatment. All patient information is confidential and only obtained, used or disclosed as necessary to perform job duties including reporting as required. We do not tolerate breaches in confidential information and proactively safeguard patient information in keeping with The Health Insurance Portability and Accountability Act (HIPAA) requirements."[16]

45. Plaintiff and Class Members, as current and former patients of Corewell and BACO, relied on these promises and on these sophisticated entities to keep their sensitive Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Patients, in general, demand security to safeguard their Private Information, especially when PHI and other sensitive Private Information is involved.

---

[15] *Id.*

[16] Code of Conduct, Beaumont ACO, available at https://www.beaumont-aco.org/docs/default-source/default-document-library/aco-code-of-conduct-04302014-_2_.pdf?sfvrsn=5d768156_2 (last accessed Jan. 8, 2024) (attached as **Exhibit I** hereto).

The Data Breach

46. On an undisclosed date, HEC "became aware of suspicious activity potentially involving its network and promptly began an investigation," which determined that between July 14, 2023 and July 23, 2023, HEC's "systems were accessed by an unknown actor" and "during this time certain files were copied."[17] The unknown actor obtained files containing information about Corewell, BACO, and other healthcare entities' current and former patients.[18]

47. HEC "recently confirmed that the protected health information of 4,452,782 individuals has been exposed and potentially stolen."[19] "[M]ore than one million Michigan residents" have been affected by the Data Breach.[20]

48. Through its investigation into the Data Breach, HEC discovered that the information affected by the Data Breach included names, addresses, dates of birth, Social Security numbers, Taxpayer Identification numbers, medical record numbers, medical information (including but not limited to diagnoses, diagnosis codes, mental/physical conditions, prescription information, and provider names and

---

[17] *See* Notice of Data Breach, *supra* note 1.
[18] *Id.*
[19] *See HealthEC Data Breach Affects Almost 4.5 Million Individuals*, *supra* note 5.
[20] *Second Corewell Health Data Breach Exposes Info of One Million Michigan Patients*, Michigan Department of Attorney General (Dec. 26, 2023), https://www.michigan.gov/ag/news/press-releases/2023/12/26/second-corewell-health-data-breach-exposes-info-of-one-million-michigan-patients (last accessed Jan. 5, 2024) (attached as **Exhibit J** hereto).

locations), health insurance information (including but not limited to beneficiary numbers, subscriber numbers, Medicaid/Medicare identifications), and/or billing and claims information (including but not limited to patient account numbers, patient identification numbers, and treatment cost information) that Defendants collected and maintained as part of their provision of services.[21]

49. Though the data breach occurred sometime between July 14, 2023 and July 23, 2023, HEC waited until October 26, 2023, more than three months later, to being notifying its clients that their patients' Private Information was in the hands of cybercriminals.[22] HEC also waited until December 22, 2023, five months after the Data Breach, to mail notice letters to impacted persons.[23]

50. Generally speaking, a ransomware attack, like that experienced by Defendants is a type of cyberattack that is frequently used to target companies due to the sensitive patient data they maintain.[24] In a ransomware attack the attackers use software to encrypt data on a compromised network, rendering it unusable and

---

[21] *See* Notice of Data Breach, *supra* note 1.
[22] *Id.*
[23] *See Second Corewell Health Data Breach Exposes Info of One Million Michigan Patients*, *supra* note 20 ("Notice letters were mailed to impacted persons by HealthEC on December 22, 2023.").#
[24] *Ransomware warning: Now attacks are stealing data as well as encrypting it*, available at https://www.zdnet.com/article/ransomware-warning-now-attacks-are-stealing-data-as-well-as-encrypting-it/ (last accessed Jan. 5, 2024) (attached as **Exhibit K** hereto).

demanding payment to restore control over the network.[25]

51. Companies should treat ransomware attacks as any other data breach incident because ransomware attacks don't just hold networks hostage, "ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[26] As cybersecurity expert Emisoft warns, "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence […] the initial assumption should be that data may have been exfiltrated."

52. An increasingly prevalent form of ransomware attack is the "encryption+exfiltration" attack in which the attacker encrypts a network and exfiltrates the data contained within.[27] In 2020, over 50% of ransomware attackers exfiltrated data from a network before encrypting it.[28] Once the data is exfiltrated from a network, its confidential nature is destroyed and it should be "assume[d] it

---

[25] *Ransomware: The Data Exfiltration and Double Extortion Trends*, available at https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends (last accessed Jan. 5, 2024) (attached as **Exhibit L** hereto).
[26] *The chance of data being stolen in a ransomware attack is greater than one in ten*, available at https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/ (last accessed Jan. 5, 2024) (attached as **Exhibit M** hereto).
[27] *2020 Ransomware Marketplace Report*, available at https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report (last accessed Jan. 5, 2024) (attached as **Exhibit N** hereto).
[28] *Ransomware FAQs*, available at https://www.cisa.gov/stopransomware/ransomware-faqs (last accessed Jan. 5, 2024) (attached as **Exhibit O** hereto).

will be traded to other threat actors, sold, or held for a second/future extortion attempt."[29] And even where companies pay for the return of data attackers often leak or sell the data regardless because there is no way to verify copies of the data are destroyed.[30]

53. Upon information and belief, the cyberattack was targeted at Defendants, due to their status as entities in the healthcare industry that collect, create, and maintain Private Information on their computer networks and/or systems.

54. Upon information and belief, Plaintiff's and Class Members' Private Information was illicitly acquired and was thus compromised in the Data Breach.

55. The files containing Plaintiff's and Class Members' Private Information, that were targeted and stolen from Defendants, included their PII and/or PHI.

56. Because of this targeted cyberattack, data thieves were able to gain access to and obtain data from Defendants that included the Private Information of Plaintiff and Class Members.

57. As evidenced by the Data Breach's occurrence, the Private Information contained in Defendants' networks and systems was not properly

[29] *Id.*
[30] *Id.*

encrypted. Had the information been properly encrypted, the data thieves would have exfiltrated only unintelligible data.

58. Plaintiff further believes that his Private Information and that of Class Members was or soon will be published to the dark web, where it will be available to purchase, because that is the *modus operandi* of cybercriminals.

59. Defendants had obligations created by the FTC Act, HIPAA, contract, state and federal law, common law, and industry standards to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

Data Breaches Are Preventable

60. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

61. Defendants could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing Private Information.

62. To prevent and detect cyber-attacks and/or ransomware attacks Defendants could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- Implement an awareness and training program. Because end users are targets, patients and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or

compression/decompression programs, including the AppData/ LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[31]

63. To prevent and detect cyber-attacks or ransomware attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

[31] *Id.* at 3-4.

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].[32]

64. Given that Defendants were storing the Private Information of Corewell and BACO's current and former patients, Defendants could and should have implemented all of the above measures to prevent and detect cyberattacks.

65. The occurrence of the Data Breach indicates that Defendants failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and, upon information and belief, the exposure of the

[32] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at: https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Jan. 5, 2024) (attached hereto as **Exhibit P**).

Private Information of over 4.4 million individuals, including that of Plaintiff and Class Members.[33]

Defendants Acquire, Collect, and Store Patients' Private Information

66. Defendants acquire, collect, and store a massive amount of Private Information on Corewell and BACO's patients, former patients and other personnel.

67. As a condition of obtaining medical services as Corewell and BACO's patients, Defendants require that patients entrust them with highly sensitive personal information.

68. HEC provided services to Defendants Corewell and BACO, which involved Corewell and BACO sharing Plaintiffs' and Class Members' Private Information with HEC.

69. By obtaining, collecting, and using Plaintiff's and Class Members' Private Information, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

70. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and would not have entrusted it to Defendants absent a promise to safeguard that information.

[33] *See Health EC Data Breach Affects Almost 4.5 Million Individuals*, *supra* note 5.

71. Plaintiff and the Class Members relied on Defendants to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Defendants Knew or Should Have Known of the Risk Because Healthcare Entities in Possession of Private Information Are Particularly Suspectable to Cyber Attacks

72. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting healthcare entities that collect and store Private Information, like Defendants, preceding the date of the breach.

73. Data breaches, including those perpetrated against healthcare entities that store Private Information in their systems, have become widespread.

74. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[34]

75. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine

[34] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022), available at https://notified.idtheftcenter.org/s/ (last accessed Jan. 5, 2024) (attached as **Exhibit Q** hereto).

(974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendants knew or should have known that their electronic records would be targeted by cybercriminals.

76. Defendants knew and understood unprotected or exposed Private Information in the custody of healthcare entities, like Defendants, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that Private Information through unauthorized access.

77. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendants' data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

78. Indeed, cyber-attacks, such as the one experienced by Defendants, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and

prepared for, a potential attack. As one report explained, smaller entities that store Private Information are "attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[35]

79. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

80. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

81. The ramifications of Defendants' failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

82. As entities in the healthcare industry in custody of current and former patients' Private Information, Defendants knew, or should have known, the importance of safeguarding Private Information entrusted to them by Plaintiff and Class Members, and of the foreseeable consequences if their data security systems

[35] Report on CommonSpirit Ransomware Attack (2023), https://classactionsreporter.com/commonspirit-ransomware-attack-and-data-breach-class-action-2/ (last accessed Jan. 5, 2024) (attached as **Exhibit R** hereto).

were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

Value of Private Information

83. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[36] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[37]

84. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[38]

85. For example, PII can be sold at a price ranging from $40 to $200.[39]

---

[36] 17 C.F.R. § 248.201 (2013).
[37] *Id.*
[38] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Jan. 5, 2024) (attached as **Exhibit S** hereto).
[39] *Here's How Much Your Personal Information Is Selling for on the Dark Web*,

Criminals can also purchase access to entire company data breaches from $900 to $4,500.[40]

86. PII can sell for as much as $363 per record according to the Infosec Institute.[41] PII is particularly valuable because criminals can use it to target victims with frauds and scams.

87. Identity thieves use stolen PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

88. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[42]

89. According to account monitoring company LogDog, medical data

---

Experian (Dec. 6, 2017), available at: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Jan. 5, 2024) (attached as **Exhibit T** hereto).

[40] *In the Dark*, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Jan. 5, 2024) (attached as **Exhibit U** hereto).

[41] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Jan. 5, 2024) (attached as **Exhibit V** hereto).

[42] Medical I.D. Theft, efraudprevention.net, https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected (last visited Jan. 5, 2024) (attached as **Exhibit W** hereto).

sells for $50 and up on the Dark Web.[43]

90. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. Upon information and belief, the information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

91. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[44]

92. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

93. The fraudulent activity resulting from the Data Breach may not come

---

[43] *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), available at: https://news.sophos.com/en-us/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/ (last accessed Jan. 5, 2024) (attached as **Exhibit X** hereto).

[44] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World (Feb. 6, 2015), available at: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Jan. 5, 2024) (attached as **Exhibit Y** hereto).

to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[45]

Defendants Failed to Comply With FTC Guidelines

94. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

95. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand

[45] *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: https://www.gao.gov/assets/gao-07-737.pdf (last visited Jan. 5, 2024) (attached as **Exhibit Z** hereto).

their network's vulnerabilities; and implement policies to correct any security problems.[46]

96. The guidelines also recommend that healthcare businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[47]

97. The FTC further recommends that healthcare companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

98. The FTC has brought enforcement actions against healthcare entities for failing to protect patient data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential patient data as an unfair act or practice prohibited by Section 5 of

---

[46] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016), available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Jan. 5, 2024) (attached as **Exhibit AA** hereto).

[47] *Id.*

the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

99. These FTC enforcement actions include actions against healthcare providers like Defendants. *See, e.g.*, *In the Matter of LabMd, Inc., A Corp*, 2016-2 Trade Cas. ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

100. Defendants failed to properly implement basic data security practices.

101. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

102. Upon information and belief, Defendants were at all times fully aware of their obligation to protect patients' Private Information. Defendants were also aware of the significant repercussions that would result from their failure to do so.

Defendants Failed to Comply With HIPAA Guidelines

103. Defendants are covered entities under HIPAA (45 C.F.R. § 160.102) and are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security

Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

104. Defendants are subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[48] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

105. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

106. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

107. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

108. "Electronic protected health information" is "individually identifiable health information . . . that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

[48] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

109. HIPAA's Security Rule requires Defendants to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

110. HIPAA also requires Defendants to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendants are required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

111. HIPAA and HITECH also obligated Defendants to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that

are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

112. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendants to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[49]

113. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

114. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

115. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§

[49] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added) (last visited Jan. 5, 2024) (attached as **Exhibit BB** hereto).

164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule."[50] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI."[51]

Defendants Fail to Comply With Industry Standards

116. As noted above, experts studying cyber security routinely identify healthcare entities in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

117. Several best practices have been identified that, at a minimum, should be implemented by healthcare entities in possession of Private Information, like Defendants, including but not limited to: educating all employees; strong

[50] US Department of Health & Human Services, Security Rule Guidance Material, http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last visited Jan. 5, 2024) (attached as **Exhibit CC** hereto).

[51] US Department of Health & Human Services, Guidance on Risk Analysis, https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (last visited Jan. 5, 2024) (attached as **Exhibit DD** hereto).

passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendants failed to follow these industry best practices, including a failure to implement multi-factor authentication.

118. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendants failed to follow these cybersecurity best practices, including failure to train staff.

119. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

120. These foregoing frameworks are existing and applicable industry

standards in the healthcare industry, and upon information and belief, Defendants failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

COMMON INJURIES & DAMAGES

121. As a result of Defendants' ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of illicit actors, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their Private Information; (e) invasion of privacy; and (f) the continued risk to their Private Information, which remains in the possession of Defendants, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

The Data Breach Increases Victims' Risk of Identity Theft

122. Plaintiff and Class Members are at a heightened risk of identity theft for years to come.

123. The unencrypted Private Information of Class Members will end up

for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted Private Information may fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the Private Information of Plaintiff and Class Members.

124. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

125. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity—or track the victim to attempt other crimes against the individual to obtain more data to perfect a crime.

126. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone

calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

127. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[52]

128. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

129. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other

[52] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/ (last visited on Jan. 5, 2024) (attached hereto as **Exhibit EE**).

unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

130. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiff and the other Class Members.

131. Thus, even if certain information (such as Social Security numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

132. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss of Time to Mitigate Risk of Identity Theft and Fraud

133. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and

otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

134. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must monitor their financial accounts for many years to mitigate the risk of identity theft.

135. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as monitoring their accounts for fraudulent activity and checking their credit reports for unusual activity.

136. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[53]

137. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit

[53] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf (last visited Jan. 5, 2024) (attached hereto as **Exhibit FF**).

bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[54]

138. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[55]

Diminution Value of Private Information

139. PII and PHI are valuable property rights.[56] Their value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

---

[54] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited Jan. 5, 2024) (attached as **Exhibit GG** hereto).

[55] *See supra* n.53 at p.2.

[56] *See, e.g.*, Randall T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private Information") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

140. An active and robust legitimate marketplace for Private Information exists. In 2019, the data brokering industry was worth roughly $200 billion.[57]

141. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[58,59]

142. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[60]

143. Conversely sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[61]

144. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized

---

[57] Los Angeles Times, Column: Shadowy data brokers make the most of their invisibility cloak, David Lazarus (Nov. 5, 2019), available at https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited Jan. 5, 2024) (attached as **Exhibit HH** hereto).

[58] *See* https://datacoup.com/ (last visited Jan. 5, 2024) (attached as **Exhibit II** hereto).

[59] *See* https://digi.me/about-us (last visited Jan. 5, 2024) (attached as **Exhibit JJ** hereto).

[60] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Jan. 5, 2024) (attached as **Exhibit KK** hereto).

[61] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Jan. 5, 2024) (attached as **Exhibit LL** hereto).

release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

145. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. Upon information and belief, the information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

146. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

147. The fraudulent activity resulting from the Data Breach may not come to light for years.

148. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result

of a breach.

149. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' networks, amounting to over a million individuals' detailed personal information, upon information and belief, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

150. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

151. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes, e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

152. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her personal

information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

153. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

154. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendants' Data Breach.

Loss of the Benefit of the Bargain

155. Furthermore, Defendants' poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendants and/or its agents for the provision of medical services, Plaintiff and other reasonable consumers understood and expected that they were, in part, paying for the service and necessary data security to protect their Private Information, when in fact, Defendants did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendants.

PLAINTIFF DINNING'S EXPERIENCE

156. Plaintiff Douglas Dinning has received healthcare services from

Defendants.

157. In order to receive medical services as a patient, Plaintiff Dinning was required to provide his Private Information to Defendants.

158. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's Private Information in their systems.

159. Plaintiff Dinning is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff would not have entrusted his Private Information to Defendants had he known of Defendants' lax data security policies.

160. Upon information and belief, Plaintiff's PII and/or PHI was improperly accessed and obtained by unauthorized third parties in the Data Breach.

161. Plaintiff received two notice letters from HealthEC dated December 22, 2023 informing him that his Private Information, including his name, address, date of birth, Social Security Number, medical information, health insurance information, and billing or claims information, was compromised in the Data Breach. One noted that it was being sent in connection with Defendant HealthEC's relationship with Defendant Corewell Health and the other in connection with

Defendant HealthEC's relationship with Defendant Beaumont ACO.[62]

162. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including monitoring his accounts for fraudulent activity and checking his credit reports for unusual activity. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

163. Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

[62] *See* Exhibits MM & NN.

164. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

165. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

166. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

167. Plaintiff Dinning has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

168. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

169. Specifically, Plaintiff proposes the following class definitions, subject to amendment as appropriate:

Nationwide Class
All persons in the United States whose PII and/or PHI was compromised as a result of the Data Breach (the "Class").

Michigan Subclass
All persons in the state of Michigan whose PII and/or PHI was compromised

as a result of the Data Breach (the "Michigan Subclass").

170. Excluded from the Classes are Defendants and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

171. Plaintiff reserves the right to modify or amend the definition of the proposed Classes, as well as add subclasses, before the Court determines whether certification is appropriate.

172. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

173. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Although the precise number of such persons is currently unknown to Plaintiff and exclusively in the possession of Defendants, according to the Michigan Department of Attorney General, more than 1 million Michigan residents were impacted in the Data Breach.[63] Thus, the Class is sufficiently numerous to warrant certification.

174. Commonality. There are questions of law and fact common to the

[63] *See Second Corewell Health Data Breach Exposes Info of One Million Michigan Patients*, *supra* note 20.

Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants engaged in the conduct alleged herein;

b. Whether Defendants' conduct violated the FTCA and/or HIPAA;

c. When Defendants learned of the Data Breach;

d. Whether Defendants' response to the Data Breach was adequate;

e. Whether Defendants unlawfully lost or disclosed Plaintiff's and Class Members' Private Information;

f. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

g. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

h. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

i. Whether Defendants owed a duty to Class Members to safeguard their Private Information;

j. Whether Defendants breached their duty to Class Members to safeguard their Private Information;

k. Whether hackers obtained Class Members' Private Information via the

Data Breach;

l. Whether Defendants had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;

m. Whether Defendants breached their duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

n. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

o. What damages Plaintiff and Class Members suffered as a result of Defendants' misconduct;

p. Whether Defendants' conduct was negligent;

q. Whether Defendants were unjustly enriched;

r. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;

s. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

t. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

175. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class

Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Defendants. Plaintiff is advancing the same claims and legal theories on behalf of himself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

176. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

177. Predominance. Defendants have engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

178. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are

likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

179. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Defendants have acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

180. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to the names and addresses and/or email addresses of Class Members affected by the Data Breach.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class against all Defendants)

181. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

182. Defendants require their patients, including Plaintiff and Class Members, to submit non-public Private Information in the ordinary course of providing medical services.

183. Defendants gathered and stored the Private Information of Plaintiff and Class Members as part of their business of soliciting services to their patients, which solicitations and services affect commerce.

184. Plaintiff and Class Members entrusted Defendants with their Private Information with the understanding that Defendants would safeguard their information.

185. Defendants had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information were wrongfully disclosed.

186. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendants had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to implement processes by which they could detect a breach of their

security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

187. Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

188. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

189. Defendants owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

190. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and their

patients. That special relationship arose because Plaintiff and the Class entrusted Defendants with their confidential Private Information, a necessary part of being patients of Defendants.

191. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Private Information.

192. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiff or the Class.

193. Defendants also had a duty to exercise appropriate clearinghouse practices to remove former patients' Private Information it was no longer required to retain pursuant to regulations.

194. Moreover, Defendants had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

195. Defendants had and continue to have a duty to adequately disclose that the Private Information of Plaintiff and the Class within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

196. Defendants breached their duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failure to periodically ensure that their email systems had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

f. Failing to remove former patients' Private Information it was no longer required to retain pursuant to regulations;

g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

h. Failing to secure their stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

197. Defendants violated Section 5 of the FTC Act and HPAA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendants' conduct

was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

198. Plaintiff and the Class are within the class of persons that the FTC Act and HIPAA were intended to protect.

199. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act and HIPAA were intended to guard against.

200. Defendants' violation of Section 5 of the FTC Act and HIPAA constitutes negligence.

201. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

202. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

203. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

204. Defendants have full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if the Private Information were wrongfully disclosed.

205. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendants' systems.

206. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

207. Plaintiff and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendants' possession.

208. Defendants were in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

209. Defendants' duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties

are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

210. Defendants have admitted that the Private Information of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

211. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and the Class, the Private Information of Plaintiff and the Class would not have been compromised.

212. There is a close causal connection between Defendants' failure to implement security measures to protect the Private Information of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The Private Information of Plaintiff and the Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

213. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with

attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

214. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

215. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in their continued possession.

216. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

217. Defendants' negligent conduct is ongoing, in that they still hold the Private Information of Plaintiff and Class Members in an unsafe and insecure manner.

218. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiff and the Class against all Defendants)

219. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

220. Plaintiff and Class Members were required to provide their Private Information to Defendants as a condition of receiving medical services from Defendants.

221. Plaintiff and the Class entrusted their Private Information to Defendants. In so doing, Plaintiff and the Class entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or

stolen.

222. Implicit in the agreement between Plaintiff and Class Members and the Defendants to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the Private Information only under conditions that kept such information secure and confidential.

223. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendants, on the other, is demonstrated by their conduct and course of dealing.

224. Defendants solicited, offered, and invited Plaintiff and Class Members to provide their Private Information as part of Defendants' regular business practices. Plaintiff and Class Members accepted Defendants' offers and provided their Private Information to Defendants.

225. In accepting the Private Information of Plaintiff and Class Members, Defendants understood and agreed that they were required to reasonably safeguard

the Private Information from unauthorized access or disclosure.

226. On information and belief, at all relevant times Defendants promulgated, adopted, and implemented written privacy policies whereby they expressly promised Plaintiff and Class Members that they would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

227. On information and belief, Defendants further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' Private Information would remain protected.

228. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations and were consistent with industry standards.

229. Plaintiff and Class Members paid money to Defendants with the reasonable belief and expectation that Defendants would use part of their earnings to obtain adequate data security. Defendants failed to do so.

230. Plaintiff and Class Members would not have entrusted their Private Information to Defendants in the absence of the implied contract between them and Defendants to keep their information reasonably secure.

231. Plaintiff and Class Members would not have entrusted their Private Information to Defendants in the absence of their implied promise to monitor their

computer systems and networks to ensure that they adopted reasonable data security measures.

232. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendants.

233. Defendants breached the implied contracts they made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

234. As a direct and proximate result of Defendants' breach of the implied contracts, Plaintiff and Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain.

235. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

236. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, e.g., (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT III
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class against Defendants BACO and Corewell)

237. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

238. This claim is brought by Plaintiff on behalf of all Class Members who provided their PII and PHI to Defendants BACO and Corewell.

239. Plaintiff and the other Class Members gave BACO and Corewell their PII and PHI in confidence, believing that BACO and Corewell would protect that information. Plaintiff and the other Class Members would not have provided BACO and Corewell with this information had they known it would not be adequately protected. BACO and Corewell's acceptance and storage of Plaintiff's and the other Class Members' PII and PHI created a fiduciary relationship between BACO and Corewell on the one hand, and Plaintiff and the other Class members, on the other hand. In light of this relationship, BACO and Corewell must act primarily for the benefit of their patients, which includes safeguarding and protecting Plaintiff's and the other Class members' PII and PHI.

240. Due to the nature of the relationship between BACO and Corewell on the one hand, and Plaintiff and the other Class Members, on the other hand, Plaintiffs and the other Class Members were entirely reliant upon BACO and Corewell to ensure that their PII and PHI was adequately protected. Plaintiff and

the other Class Members had no way of verifying or influencing the nature and extent of BACO and Corewell's or their vendors' data security policies and practices, and BACO and Corewell were in an exclusive position to guard against the Data Breach.

241. BACO and Corewell have a fiduciary duty to act for the benefit of Plaintiff and the other Class Members upon matters within the scope of their relationship. They breached that duty by contracting with companies that failed to properly protect the integrity of the systems containing Plaintiff's and the other Class Members' PII and PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiff's and the other Class Members' PII and PHI that they collected.

242. As a direct and proximate result of BACO and Corewell's breaches of their fiduciary duties, Plaintiff and the other Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII and PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII and PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII and PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required

to prevent, detect, and repair the impact of the PII and PHI compromised as a result of the Data Breach; (vii) loss of potential value of their PII and PHI; and (viii) overpayment for the services that were received without adequate data security.

COUNT IV
Violation of the Michigan Consumer Protection Act
(On Behalf of Plaintiff and the Michigan Subclass against all Defendants)

243. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein and brings this count on behalf of himself and the Michigan Subclass (the "Class" for the purposes of this count).

244. Plaintiff is authorized to bring this claim under Mich. Comp. Laws § 445.911.

245. The Michigan Consumer Protection Act ("MCPA"), Mich. Comp. Laws § 445.901, *et seq.*, prohibits "unfair, unconscionable, or deceptive methods, acts, or practices in the conduct of trade or commerce[.]" Mich. Comp. Laws § 445.903(1).

246. As described in this Complaint, Defendants have engaged in the following unfair, unconscionable, and deceptive trade practices that are made unlawful under the MCPA, Mich. Comp. Laws § 445.903(1):

> (c) Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have or that a person has sponsorship, approval, status, affiliation, or connection that she or she does not have;

. . .

(e) Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or mode, if they are of another;

. . .

(s) Failing to reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer; and

. . .

(cc) Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive manner.

247. Defendants' deceptive acts or practices in the conduct of commerce include, but are not limited to:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the industry, which were direct and proximate causes of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information, including but not limited to duties imposed by the FTC Act, which were direct and proximate causes of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff's and Class Members' Private Information;

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information; and

h. Failing to promptly and adequately notify Plaintiff and the Class that their Private Information was accessed by unauthorized persons in the Data Breach.

248. Defendants are engaged in, and their acts and omissions affect, trade and commerce. Defendants' relevant acts, practices, and omissions complained of in this action were done in the course of Defendants' business of marketing, offering for sale, and selling goods and services throughout the United States.

249. Defendants had exclusive knowledge of material information regarding their deficient security policies and practices, and regarding the security of Plaintiff's and Class Members' Private Information. This exclusive knowledge includes, but is not limited to, information that Defendants received through internal and other non-public audits and reviews that concluded that Defendants' security policies were substandard and deficient, and that Plaintiff's and Class Members' Private Information and other data was vulnerable.

250. Defendants had exclusive knowledge about the extent of the Data

Breach, including during the days, weeks, and months following the Data Breach.

251. Defendants also had exclusive knowledge about the length of time that it maintained individuals' Private Information after they stopped using services that necessitated the transfer of that Private Information to Defendants.

252. Defendants failed to disclose, and actively concealed, the material information they had regarding Defendants' deficient security policies and practices, and regarding the security of the sensitive PII and PHI. For example, even though Defendants have long known, through internal audits and otherwise, that their security policies and practices were substandard and deficient, and that Plaintiff's and Class Members' Private Information was vulnerable as a result, Defendants failed to disclose this information to, and actively concealed this information from, Plaintiff, Class Members and the public. Defendants also did not disclose, and actively concealed, information regarding the extensive length of time that they maintain former patients' Private Information and other records. Likewise, during the days and weeks following the Data Breach, Defendants failed to disclose, and actively concealed, information that they had regarding the extent and nature of the Data Breach.

253. Defendants had a duty to disclose the material information that they had because, inter alia, they had exclusive knowledge of the information, they actively concealed the information, and because Defendants were in a fiduciary

position by virtue of the fact that Defendants collected and maintained Plaintiff's and Class Members' PII and PHI.

254. Defendants' representations and omissions were material because they were likely to deceive reasonable individuals about the adequacy of Defendants' data security and their ability to protect the confidentiality of current and former patients' Private Information.

255. Had Defendants disclosed to Plaintiff and the Class that their data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business without adopting reasonable data security measures and complying with the law. Instead, Defendants received, maintained, and compiled Plaintiff's and Class Members' Private Information without advising that Defendants' data security practices were insufficient to maintain the safety and confidentiality of their Private Information.

256. Accordingly, Plaintiff and Class Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

257. Defendants' practices were also contrary to legislatively declared and public policies that seek to protect data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected in laws, such as HIPAA and the FTC Act.

258. The injuries suffered by Plaintiff and the Class greatly outweigh any potential countervailing benefit to patients/consumers or to competition and are not injuries that Plaintiff and the Class should have reasonably avoided.

259. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiff and the Class as a direct result of Defendants' deceptive acts and practices as set forth herein include, without limitation: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

260. Plaintiff and the Class seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring Defendants from disclosing their Private Information without their consent; reasonable attorneys' fees and costs; and any

other relief that is just and proper.

COUNT V
Violation of the Michigan Data Breach Notification Statute
(On Behalf of Plaintiff and the Class against all Defendants)

261. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein and brings this count on behalf of himself and the Michigan Subclass (the "Class" for the purposes of this count).

262. Plaintiff is authorized to bring this claim under Mich. Comp. Laws § 445.73(13).

263. Defendants are corporations that own, maintain, and record PII and PHI, and computerized data including PII and PHI, about their current and former patients, including Plaintiff and Class Members.

264. Defendants are in possession of PII and PHI belonging to Plaintiff and Class Members and are responsible for reasonably safeguarding that PII and PHI consistent with the requirements of Mich. Comp. Laws § 445.72.

265. Defendants failed to safeguard, maintain, and dispose of, as required, the PII within their possession, custody, or control as discussed herein, which they were required to do by Michigan law.

266. Defendants, knowing and/or reasonably believing that Plaintiff's and Class Members' PII and PHI was acquired by unauthorized persons during the Data

Breach, failed to provide reasonable and timely notice of the Data Breach to Plaintiff and Class Members, as required by Mich. Comp. Laws § 445.72(1), (4).

267. As a result of Defendants' failure to reasonably safeguard Plaintiff's and Class Members' PII, and the failure to provide reasonable and timely notice of the Data Breach to Plaintiff and Class Members, Plaintiff and the Class have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PII in Defendants' possession, and are entitled to damages in an amount to be proven at trial.

COUNT VI
Unjust Enrichment
(On Behalf of Plaintiff and the Class against all Defendants)

268. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

269. This count is pleaded in the alternative to Plaintiff's breach of implied contract claim above (Count II).

270. Plaintiff and Class Members conferred a monetary benefit on Defendants. Specifically, they paid for services from Defendants and/or their agents and in so doing also provided Defendants with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendants the services that were the subject of the transaction and should have had their Private Information protected with adequate data security.

271. Defendants knew that Plaintiff and Class Members conferred a benefit on them in the form of their Private Information as well as payments made on their behalf as a necessary part of their receiving healthcare services. Defendants appreciated and accepted that benefit. Defendants profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

272. Upon information and belief, Defendants fund their data security measures entirely from their general revenue, including payments on behalf of or for the benefit of Plaintiff and Class Members.

273. As such, a portion of the payments made for the benefit of or on behalf of Plaintiff and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendants.

274. Defendants, however, failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not provide adequate data security in return for the benefit Plaintiff and Class Members provided.

275. Defendants would not be able to carry out an essential function of their regular business without the Private Information of Plaintiff and Class Members and derived revenue by using it for business purposes. Plaintiff and Class Members expected that Defendants or anyone in Defendants' position would use a portion of

that revenue to fund adequate data security practices.

276. Defendants acquired the Private Information through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

277. If Plaintiff and Class Members knew that Defendants had not reasonably secured their Private Information, they would not have allowed their Private Information to be provided to Defendants.

278. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendants instead calculated to increase their own profit at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to their own profit. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' decision to prioritize their own profits over the requisite security and the safety of their Private Information.

279. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money wrongfully obtained Plaintiff and Class Members, because Defendants failed to implement appropriate data management and security measures that are mandated by industry standards.

280. Plaintiff and Class Members have no adequate remedy at law.

281. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

282. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

283. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendants'

services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and his counsel to represent the Class and Michigan Subclass;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

C. For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to patient data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

D. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. Prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. Requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. Requiring Defendants to delete, destroy, and purge the Private Information of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. Requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;

v. Prohibiting Defendants from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;

vi. Requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. Requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. Requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;

ix. Requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

x. Requiring Defendants to conduct regular database scanning and securing checks;

xi. Requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. Requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. Requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiv. Requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. Requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; and

xvi. Requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and

xvii. For a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment.

E. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

F. Ordering Defendants to pay for not less than ten years of credit monitoring services for Plaintiff and the Class;

G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

H. For an award of punitive damages, as allowable by law;

I. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

J. Pre- and post-judgment interest on any amounts awarded; and

K. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: January 9, 2024

Respectfully submitted,

/s/ E. Powell Miller .

E. Powell Miller (P39487)
Emily E. Hughes (P68724)
Mitchell J. Kendrick (P83705)
THE MILLER LAW FIRM
950 W. University Drive, Suite 300
Rochester, MI 48307
T: (248) 841-2200
epm@millerlawpc.com
eeh@millerlawpc.com
mjk@millerlawpc.com

Attorneys for Plaintiff and Putative Class